

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of  
*(Briefly describe the property to be searched  
 or identify the person by name and address)*  
 ACCOUNTS THAT ARE STORED AT PREMISES  
 CONTROLLED BY GOOGLE

Case No.

2:20-mj-616

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1343	Wire Fraud

The application is based on these facts:

See attached Affidavit.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Robert E. White II, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: September 4, 2020

City and state: Columbus, Ohio

  
 Elizabeth A. Preston Deavers  
 United States Magistrate Judge


UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF OHIO  
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF:

ACCOUNTS THAT ARE STORED AT  
PREMISES CONTROLLED BY GOOGLE

Case No.

2:20-mj-616

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Robert E. White II, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the FBI assigned to the Cincinnati Division, and I have been a Special Agent since September 2002. Before becoming a Special Agent with the FBI, I was an officer in the United States Navy for approximately twelve years. My duties included surface warfare, electronic warfare, and cryptologic operations. I have my Bachelor's Degree in Computer Science and my Master's Degree in Business Administration.

2. During my career as a Special Agent, I conducted numerous public corruption, counterintelligence, and cyber investigations. I have participated in various investigations involving computer-related offenses. I have executed numerous search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. I have experience using sophisticated investigative techniques to include electronic surveillance, GPS tracking devices, telephone tracking, and wiretaps.

3. I, along with other agents and officers from the FBI, the Columbus Division of Police (CPD), the Ohio Bureau of Criminal Investigation (BCI), and the Ohio Auditor of State (AOS), have been investigating corruption in the Columbus Division of Police Department's

Vice Unit involving CPD Vice Unit Detectives Steven G. ROSSER and Whitney R. LANCASTER. Over the course of this investigation, I have become familiar with the organization and structure of the CPD Vice Unit and the nature and scope of the CPD Vice Unit's duties.

4. The facts outlined in this affidavit come from my observations, my training, experience with this investigation, and investigative reports and information provided to me by other federal and state law enforcement officers and witnesses. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on the facts outlined in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1341 (mail fraud), and 18 U.S.C. § 1343 (wire fraud) have been committed by Columbus Police Department Vice Unit Detectives Steven G. ROSSER and Whitney R. LANCASTER. There is probable cause to believe that the location information described in Attachment B will constitute evidence of these criminal violations, and corroborate witness information.

6. The accounts (hereinafter referred to as the "SUBJECT ACCOUNTS") are associated with the following identifiers:

Phone number: (614)307-5882, IMEI: 353797087246450, MEID: 35379708724645;

Phone number: (614)687-1159, IMEI: 353797088515030, IMSI: 311480293851318;

Phone number: (614)756-9477, IMEI: 356771083909776, IMSI: 310410045434583;

Phone number: (614)906-0222, ESN/MSN: 089594804007870547, IMSI: 310120237623211,

email addresses: ostranderauto@gmail.com, liquidatorsunlimitedinc@gmail.com,

whit5polo@gmail.com, and jcable77@yahoo.com, deana.steve@aol.com,

srosser17@yahoo.com. The SUBJECT ACCOUNTS are maintained and controlled by Google LLC (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

7. The information to be searched is described in the following paragraphs and Attachment A. Attachment B describes the matters and things to be searched and seized within referenced accounts and device IDs. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Provider to disclose to the government copies of the information (including the content of communications) further described in Attachment B. All statements made in Attachments A and B are adopted into this affidavit body as if fully set forth herein.

#### **BACKGROUND CONCERNING GOOGLE**

8. In my training and experience, I have learned that Google provides various online services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name Gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide necessary personal information. Therefore, the servers maintained or owned by Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the data can be used to identify the account's user or users.

9. Google has developed an operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account. Users are prompted to add a Google account when they first turn on a new Android device.

10. Based on my training and experience, I have learned that Google collects and retains location data from Android-enabled devices and from Google Apps on all devices when a Google account user has enabled Google location service. The company uses this information for location-based advertising and location-based search results. This information is derived from GPS data, cell site/cell tower information, and WiFi access points.

11. Location data can help investigators understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate anyone in possession of a device registered with a particular account. Additionally, data stored at the user's account may further indicate the account user's geographic location at a specific time (e.g., location information integrated into an image or video sent via email).

### **JURISDICTION**

12. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **PROBABLE CAUSE**

13. Steven G. ROSSER was an 19-year veteran of the Columbus Police Department, joining the police force in 2000. In 2013, after approximately 12 years as patrol officer, ROSSER was assigned as a detective in the CPD Vice Unit. ROSSER served in the Vice unit until 2019 when he was reassigned to patrol, prior to his termination on January 23, 2020.

14. Whitney R. LANCASTER was a 31-year veteran of the Columbus Police Department, joining the police force in 1987. LANCASTER served in patrol, juvenile and narcotics divisions for 11 years prior to being promoted to detective in 1998. In 2016 he was assigned to the Vice Unit. LANCASTER served in the Vice unit until 2019 when he was reassigned to patrol, prior to his termination on January 23, 2020.

15. The Columbus Police Department ("CPD") Vice Unit is charged with enforcing, among other things, prostitution-related offenses, liquor-control offenses, and conducting compliance checks in night clubs, after-hours clubs, and adult entertainment venues. Because of the nature of the offenses and the types of crimes being investigated, CPD Vice Unit detectives are given broad latitude while performing their duties.

16. On or about January 2, 2018 a water pipe at the Fort Rapids Indoor Waterpark Resort ("Fort Rapids"), located at 4560 Hilton Corporate Drive Columbus, Ohio, broke and flooded the building for about seven hours. The flooding caused severe damage and because of multiple health code violations, the building was closed indefinitely.

17. Due to the condition of the building, Columbus Fire Department (CFD) required a 24 hours/day fire watch consisting of two man shifts to be maintained on the Fort Rapids building until the required repairs were completed.

18. After several failed attempts to engage security companies, the California-based company that owned the building reached out to ROSSER to ask if he could provide 24-

hour security on the building. On January 3, 2018, CPD officers began serving special duty at Fort Rapids.

19. Special Duty refers to the hiring of an off-duty CPD officer(s) for security, traffic control or escorts within the city of Columbus. Special Duty jobs are filled on a voluntary basis and paid at a fixed hourly rate.

20. On or about January 4, 2018, ROSSER emailed the Fort Rapids representative indicating the email represented the contract between Fort Rapids and the CPD officers who would be conducting special duty at Fort Rapids. As the special duty coordinator ROSSER was responsible for insuring the watch was properly manned and providing billing invoices to the Fort Rapids representative for payment.

21. The officers working special duty are required to complete timecards detailing the dates and times that an officer was protecting the property. The Columbus Police Special Duty Invoices maintained and signed by the coordinator. The officers were paid by checks which were mailed from California to Ohio.

22. Investigators reviewed the Columbus Police Special Duty Invoices retrieved from ROSSER's CPD office, the billing invoices ROSSER submitted to the Fort Rapids representative and cashed checks. From January 3, 2018 to October 28, 2018, ROSSER received at least \$51,696 in special duty pay which included \$12,672 for duty administration. Your affiant compared ROSSER's special duty timecards to the CPD time and attendance records and discovered numerous irregularities, including:

- a. On approximately 30 occasions totaling 137 hours, ROSSER reported working Special Duty at the same time he reported working for CPD.

- b. On approximately 17 occasions ROSSER reported starting or ending a special duty shift at the same time as starting or ending a CPD shift. This is unusual given that as a vice officer, ROSSER served throughout Columbus City limits in plain clothes. As a special duty officer, he was required to be in uniform at the Fort Rapids location.
- c. On at least three occasions ROSSER reported unusually long shift times. On March 10, 2018, March 16, 2018 and April 16, 2018 ROSSER reported working shifts of 40, 34 and 24 continuous hours respectively.

23. Pursuant to a search warrant, AT&T produced call detail records for ROSSER's cell phone, number (614)756-9477. Your affiant analyzed the records and found multiple days when ROSSER claimed to be working special duty, but was not located at Fort Rapids for the full shift. For example, on February 16, 2018, ROSSER reported working special duty from 7 AM to 11 PM. He also reported working a CPD shift from 7 AM to 3 PM. AT&T cell tower records showed that from 6:14 AM to 12:53 PM, ROSSER was in northwest Columbus or in the vicinity of the CPD Vice offsite. He did not arrive at Fort Rapids in east Columbus until approximately 1:10 PM. Records showed he remained in that location until 10:55 PM. In that instance, ROSSER claimed approximately 6 hours of special duty pay while engaged in other activities away the site he was supposedly guarding.

24. Because cell phone location data is only captured when the device is actively being used, such as during a phone call or while an app communicating in the background, there are large gaps of time where the device cannot be located. Locational data collected by Google includes times when the user is not using their device and when the device is offline. The



information requested by the search warrant will used to corroborate and enhance the cell phone location data.

25. From January 3, 2018 to December 11, 2018 LANCASTER received \$90,816. Your affiant compared LANCASTER's special duty timecards to the CPD time and attendance records and discovered numerous irregularities, including:

- a. On approximately 50 occasions totaling 164 hours, LANCASTER reported working Special Duty at the same time he reported working a CPD shift.
- b. On approximately 79 occasions LANCASTER reported starting or ending a special duty shift at the same time as starting or ending a CPD shift.
- c. On 24 occasions LANCASTER reported unusually long shift times of 24 hours or longer. For example, LANCASTER reported starting a Fort Rapids shift on February 20, 2018, at 11 PM. The timesheets showed that the next five reported shifts alternated between CPD and Fort Rapids and resulted in 64 hours of continuous work. Starting March 4, 2018, LANCASTER reported working continuously for 56 hours, and starting on October 24, 2018 LANCASTER reported working continuously for 40 hours.

#### **SUBJECT ACCOUNTS/TARGETED DEVICES**

26. CPD issued ROSSER and LANCASTER cell phones to be used in the performance of their duties. In addition to the records Verizon produced pursuant to a search warrant investigators conducted a physical examination of ROSSER's device. It had the

following characteristics: Phone number: (614)307-5882, IMEI: 353797087246450, MEID: 35379708724645, Email address registered to it was jcable77@yahoo.com. LANCASTER's device had the following characteristics: Work cell phone number: (614)687-1159, IMEI: 353797088515030, and IMSI: 311480293851318.

27. In addition to the CPD issued cell phones, ROSSER carried personal devices. Pursuant to subpoenas AT&T and Facebook produced records which provided the following identifiers for ROSSER's cell phone(s): Personal phone number: (614)756-9477, IMSI: 310410045434583, IMEI: 356771083909776, Email addresses: deana.steve@aol.com, ostranderauto@gmail.com, and liquidatorsunlimitedinc@gmail.com, srosser17@yahoo.com

28. In addition to the CPD issued cell phones, LANCASTER carried personal devices. Pursuant to subpoenas Sprint, Facebook and US Postal Service produced records which provided the following identifiers for LANCASTER's cell phones: Personal phone number: (614)906-0222, Email addresses: whit5polo@gmail.com, ESN/MSN: 089594804007870547, and IMSI: 310120237623211.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

29. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Attachment B.

#### **CONCLUSION**

**ATTACHMENT A**  
**Property to Be Searched**

This warrant applies to information stored at premises owned, maintained, controlled, or operated by Google, Inc. (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California 9404 associated with the following account identifiers:

Phone number: (614)307-5882, IMEI: 353797087246450, MEID: 35379708724645;

Phone number: (614)687-1159, IMEI: 353797088515030, IMSI: 311480293851318;

Phone number: (614)756-9477, IMEI: 356771083909776, IMSI: 310410045434583;

Phone number: (614)906-0222, ESN/MSN: 089594804007870547, IMSI:

310120237623211

Email addresses: ostranderauto@gmail.com, liquidatorsunlimitedinc@gmail.com,

whit5polo@gmail.com, and jcable77@yahoo.com, deana.steve@aol.com,

srosser17@yahoo.com

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google, Inc. (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A.

**For the period January 1, 2018, to December 31, 2018:**

- All Google Account Registration Information, including:
  - Name
  - User-supplied contact information
  - Account creation timestamp and IP Address
  - List of Google services the account holder has enabled and/or accessed
- All Account Change History, including date and timestamps, including:
  - Password Change History
  - SMS Number Change/Update
- Account Login and Logout events to include IP Addresses and date/timestamps for the period
- Location History for the Subject account, including any deleted Location History records with associated date/timestamps

- Location History for any device that has logged into the Subject account
  - To include any location data whether it be in the form of GPS, WiFi or Bluetooth readings collected by above device(s) regardless if contained within user's Gmail account/location history settings.
  - To include any WiFi Access Points SSID's and MAC addresses in which the above device(s) has connected to for the aforementioned period.
- All device information associated with the account;
  - To include MAC Address
  - Readings of Altitude, Temperature, Battery Life, Movement/Speed Measurements for the period
- The following Android records:
  - Device ID, IMEI/MEID
  - Registered Date/Timestamp
  - First Check-In Date/Timestamp
  - Last Check-In Date/Timestamp
  - Last Check-In IP Address
  - Google Accounts tied to the Android device for the period
  - Android hardware information
  - Cell Carrier/Service provider
  - Apps downloaded to the device
- The following Drive records:
  - Subscriber information
  - Login and Logout IP Addresses and associated date/timestamps.

**II. Information to be seized by the government**

All information described above in Section I that constitutes evidence of violations 18 U.S.C. § 371 (conspiracy), 18 U.S.C. § 1341 (mail fraud), and 18 U.S.C. § 1343 (wire fraud) violations occurring **between January 1, 2018 and December 31, 2018**, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Criminal interference with the right to fair housing;
- (b) Willfully causing bodily injury because of the actual or perceived race or color of any person;
- (c) The location of any device that is registered to the accounts;
- (d) The identity of any person in possession of any device that is registered to the accounts;
- (e) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (f) Evidence indicating the state of mind, as it relates to the crimes under investigation, of any person in possession of any device that is registered to the accounts;

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.